MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF ALL AGENCIES

FROM: CHIEF INFORMATION OFFICERS COUNCIL
SALLY KATZEN, CHAIR & Deputy Director for Management, OMB
JAMES FLYZIK, VICE CHAIR & CIO, TREASURY

SUBJECT: Agency Interaction with GSA's Federal Computer Incident Response Capability (FedCIRC)

With this memorandum, the Chief Information Officers' (CIO) Council provides practices for CIOs to follow in fulfilling their responsibilities to protect agency information and systems and maintain a computer incident response and information sharing capability, consistent with OMB Circular A-130. We expect that agencies will implement these practices. The CIO Council's Security, Privacy, and Critical Infrastructure Committee developed the practices discussed in this memorandum in cooperation with OMB, GSA and member agencies.

The attachment to this memo describes the process that agencies should follow for appropriate coordination and interaction with GSA's Federal Computer Security Incident Response Capability (FedCIRC), to ensure that: 1) externally generated security incidents are reported to FedCIRC; 2) alerts and warnings from FedCIRC are received by responsible individuals in the agencies; and 3) when necessary, positive acknowledgment of receipt and reporting of corrective actions is provided to FedCIRC.

The importance of agency cooperation in this area cannot be overstated. As you know, security incidents, whether caused by viruses, hackers, or software bugs are becoming more common. Because of ever increasing network interconnections, such incidents are both faster moving and potentially more damaging to more organizations. The difficulties that we all faced with the "I Love You" worm earlier this year underscores this point.

When faced with externally generated security incidents, an agency should respond in a manner that both protects its own information assets and helps other organizations that might also be affected. Moreover we must have a sound government-wide process in place to issue alerts before damage becomes widespread. Understanding this need, OMB policy requires that agencies maintain a formal incident response capability and widely share information concerning common vulnerabilities and threats with other organizations.

FedCIRC was established in 1996 as the primary focal point to facilitate agency information sharing and to provide security warnings to the agencies. FedCIRC is a collaborative partnership of computer incident response and security professionals who work together to handle computer security incidents and provide security alert services to agencies. To ensure that appropriate officials in the law enforcement and national security community have timely alerts of widespread and higher level security incidents, FedCIRC has also established close relationships with other organizations such as the FBI's National Infrastructure Protection Center.

Neither OMB policy nor this memorandum should be read to preclude agencies from also participating in other information sharing arrangements. However, such other arrangements must not exclude the sharing of that information with the remainder of Federal agencies and FedCIRC.

We ask that you designate points of contact as outlined in the attachment without delay and, in the event of a computer security incident at your agency, take the actions described in that attachment. Additional information is available at FedCIRC's website (www.fedcirc.gov) or by contacting the FedCIRC Director, Mr. David Jarrell, (202) 708-5608 or by email to *djarrell@fedcirc.gov*. OMB requests that you provide point of contact information to FedCIRC not later than October 31, 2000.

Sally Katzen
Chair, CIO Council

Jim Flyzik
Vice Chair, CIO Council

Attachment

Attachment 1

1. Designating POCs

Using the format provided below, CIOs should identify primary and secondary points of contact (POC) within their organizations to interact with FedCIRC. This POC information should be periodically reviewed and updated to ensure continued timely receipt of security-related information, tools, and techniques. Two POCs should be selected from both the CIO or headquarters administrative level to receive high-level communications and the Information Systems Security Manager/Officer and systems administrator level to receive more detailed communications. Overall, each agency should designate at least four POCs at the headquarters level. Additional POCs at sub-headquarters level may also be designated. See Table 1.

Within each agency, consistent with OMB policy, CIOs should ensure that they have an effective process for reporting incidents to FedCIRC and for internal distribution of FedCIRC warnings and alerts.

Please furnish this information to fedcirc-info@fedcirc.gov or through the FedCIRC web site (*http://www.fedcirc.gov)* using the "FedCIRC Registry" selection in the main menu.

Table 1. Agency Point of Contact Information for FedCIRC

Office or Title and Name	Work Phone and Fax	E-mail address	Home phone	Pager/PIN or Cell Phone
Office of the Chief Information Officer				
Primary				
Alternate				
Security Manager/Systems Administrator – Headquarters				
Primary				
Alternate				
Security Manager/Systems Administrator – Sub-headquarters				
Primary				
Alternate				

2. How FedCIRC will interact with agency POCs

The POCs you designate will be your agency's principal recipient for all FedCIRC bulletins and advisories. The POCs will receive focused information regarding information security and cyber incidents. Again, two POCs each should be selected from either the CIO or organizational administrative level and the Information Systems Security Manager/Officer or Systems Administrator level. It is vitally important that agencies provide to FedCIRC and maintain up-to-date work and after-hours information.

CIO-level POCs

For significant incidents, FedCIRC will provide Advisories and Urgent Notices to CIO-level POCs via e-mail, facsimile or telephone to ensure the timely dissemination of critical information. These advisories and notices will provide only that level of detail necessary to identify the threat and level of severity. Attempted delivery will continue until positive acknowledgment of receipt is received by FedCIRC. CIOs will also receive Special Communications via the Extranet for Security Professionals (ESP), a secure, web-based information distribution mechanism. (Note: Instructions regarding ESP will be made available separately.)

ISSM/ISSO POCs

For all incidents, FedCIRC will provide technically detailed information to the Information Systems Security Managers (ISSM)/Officers (ISSO) and systems administrators. This information will be tailored to facilitate corrective or preventive action to counter a known threat or vulnerability.

In the event of a major cyber incident, FedCIRC may provide basic information through other communication methods such as phones and pagers.

Table 2. summarizes the various types of FedCIRC notifications and how they are transmitted to designated POCs.

Table 2. FedCIRC Notifications and their Transmission to POCs

Point of Contact	Type of Information	Method of Dissemination
Agency CIO (primary and alternate)	Time-sensitive virus or cyber attack (summaries)	Telephone, fax, cellular phone, pager. Delivery attempts continue until receipt is acknowledged.
	Special Communications, FedCIRC Advisories and Notices	Special Communications will be posted to the ESP. Advisories and Notices will be delivered via e-mail or alternative means as necessary.
Security managers and system administrators (primary and alternate)	Time-sensitive virus or cyber attack (details)	Telephone, fax, cellular phone, pager. Delivery attempts continue until receipt is acknowledged.
	FedCIRC Advisories and Notices, Incident Notes and Vulnerability Notes	FedCIRC Advisories and Notices will be delivered via e-mail. Incident Notes and Vulnerability Notes are published on the FedCIRC web page and the ESP.
	Topical technical data and routine information.	Monthly FedCIRC newsletter for security managers and system administrators.

3. When should agencies contact FedCIRC?

To ensure that significant incidents are recognized as early as possible, agency POCs should contact FedCIRC as soon as they identify security incidents with origins external to the agency. Depending on the nature and severity of the incident reported, FedCIRC will provide further guidance at the time of reporting. Timely reporting is essential to ensure that, among other things, law enforcement or national security officials can also be notified before the trail gets cold. FedCIRC works closely with the NIPC and understands the appropriate threshold for such additional reporting. Incidents may be reported via telephone, fax, or e-mail (fedcirc@fedcirc.gov). See the FedCIRC web site (*http://www.fedcirc.gov)* for telephone and fax numbers.

Note: Before an incident occurs, consistent with OMB policy, agencies should document their internal incident handling procedures and include protocols for contacting law enforcement, e.g., whether the incident is first reported to the agency Inspector General or directly to the NIPC. The policy should remove all internal obstacles to timely reporting.

4. Special Circumstances -- Reporting Corrective Action to FedCIRC

From time-to-time, OMB and other White House organizations use FedCIRC to gather summary information from the agencies regarding the impact of and corrective actions taken in response to significant or high visibility incidents, e.g., the Distributed Denial of Service Attacks and the I Love You Virus. FedCIRC will notify the agency POCs in such circumstances and the agencies may submit this information by email to fedcirc-info@fedcirc.gov.

5. How FedCIRC coordinates with other security organizations

When FedCIRC receives indications of significant incidents, e.g., multiple reports of similar incidents that indicate a widespread attack, it will notify the NIPC and, as appropriate, other FedCIRC partners such as DOD's Joint Task Force-Computer Network Defense and NSA's National Security Incident Response Center.

To ensure proper coordination of significant incidents of national importance, the National Security Council has established a Cyber Incident Working Group. FedCIRC is a member of this working group.

6. Additional information

Additional information on establishing and maintaining a computer incident response capability is located in NIST Special Publication 800-3.